

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION**

PRUDENTIAL DEFENSE SOLUTIONS, INC.,

Plaintiff,

v.

Case No. 20-11785

JAKE W. GRAHAM, MARK SHEAHAN,
and ROBERT CHARNOT,

Defendants.

**OPINION AND ORDER GRANTING IN PART PLAINTIFF'S MOTION FOR
SANCTIONS AND DIRECTING DEFENDANTS TO SHOW CAUSE AS
WHY A DEFAULT JUDGMENT SHOULD NOT BE ENTERED AGAINST THEM
UNDER FEDERAL RULES OF CIVIL PROCEDURE 37(B) AND 37(E)**

Plaintiff Prudential Defense Solutions, Inc., a private security and mobile patrol service company, brings this action asserting claims under the Michigan Uniform Trade Secrets Act ("MUTSA"), Mich. Comp. Laws § 445.1904, and the federal Defend Trade Secrets Act ("DTSA"), 18 U.S.C. § 1836(b)(1). It also brings state law claims for breach of contract, breach of fiduciary duty, and civil conspiracy. (ECF No. 15, PageID.247-60.)

Before the court is Plaintiff's "Motion for Sanctions for Defendants' Spoliation of Evidence," filed on August 23, 2021.¹ (ECF No. 82.) According to Eastern District of Michigan Local Rule 7.1(c), "[a] respondent opposing a motion must file a response, including a brief and supporting documents then available." The rules require responses to be filed within 14 days after service of most motions or 21 days after service of

¹ The court notes that Defendants have still not responded to a separate motion, Plaintiff's "Motion to Compel Deposition Testimony and the Production of Documents," despite it being filed on August 27, 2021. (ECF No. 83.)

dispositive motions. E.D. Mich. LR 7.1(e). To date, Defendants have not filed a response. The motion is therefore unopposed. For the reasons set forth below, Plaintiff's motion for sanctions will be granted in part, and the court will direct Defendants to show cause as to why sanctions—including case dispositive sanctions—are not warranted under Rule 37(b) or Rule 37(e).

I. BACKGROUND

Plaintiff alleges that Defendant Jake W. Graham, while still employed by Plaintiff, collaborated with Defendants Mark Sheahan and Robert Charnot to covertly establish a competing private security company in violation of Graham's binding noncompete agreement. It also claims that Defendants collectively misappropriated Plaintiff's proprietary information to use in their competing business.

A. Factual Background

1. Creation of a Competing Business

The following facts are either alleged in Plaintiff's complaint or otherwise established by the record. Defendant Graham began working for Prudential Security, Inc. ("PSI") in December 2012. (ECF No. 15, PageID.227.) On December 21, 2012, he signed a noncompete agreement, which for two years after termination prohibited him from competing with PSI—and Plaintiff Prudential Defense Solutions as an assignee—in various ways, including barring him from soliciting business from customers or providing private security services of his own. (*Id.*, PageID.270.) Defendant Graham worked for PSI until February 2019, thereafter becoming a vice president² of Plaintiff

² Plaintiff emphasizes that in this role, Defendant Graham "established contacts and business relationships with Plaintiff's clients and prospective clients

following PSI's corporate restructuring. (*Id.*, PageID.231; ECF No. 82, PageID.2404-05.) Defendant Graham worked for Plaintiff until July 2, 2020; Plaintiff terminated him after his alleged unlawful competitive activities were discovered. (ECF No. 82, PageID.2409; ECF No. 15, PageID.231.)

On January 30, 2020, while he still worked for Plaintiff, Defendant Graham submitted an application to the Illinois Department of Financial and Professional Regulation (IDFPR), seeking licensure in Illinois to operate a business for a "private security" company. (ECF No. 82, PageID.2406; ECF Nos. 18-3, 18-4.) Defendant Graham also sent a letter to the IDFPR urgently requesting it not contact Plaintiff because Plaintiff "would fire [him] on the spot if they knew [he] was pursuing [his] own license or were making plans to start [his] own business." (ECF No. 18-5, PageID.545.) Relatedly, in May 2020, Defendants Sheahan and Charnot engaged legal counsel to form this private security company. (ECF No. 18-7, PageID.549.) At one point, in June 2020, Defendant Sheahan emailed Defendants Graham and Charnot, noting their attorneys could suggest how to keep Defendant Graham "anonymous as long as possible, and how to protect [Graham] from a non-compete suit that might come down the road." (ECF No. 82-4, PageID.2458.)

In June 2020, Defendant Graham contacted James Howard, another vice president of Plaintiff, and requested that Howard join "Great Lakes Security," a company providing "on-site security guard and mobile patrol service[s]". (ECF No. 82, PageID.2405; ECF No. 18-2, PageID.525-26.) Howard recollected that Defendant

and acquired knowledge of and access to virtually all aspects of Plaintiff's business." (ECF No. 82, PageID.2406; ECF No.15, PageID.232.)

Graham was actively forming this company alongside Defendants Sheahan and Charnot. (ECF No. 82, PageID.2405; ECF No. 18-2, PageID.525-29.) According to Howard, Defendant Graham told him they would “have to be careful” in forming the business; Howard understood this to mean Defendant Graham meant that “[Plaintiff] would sue us as soon as it learned of the competing business entity.” (ECF No. 18-2, PageID.526.) On July 2, 2020, Plaintiff learned of Defendant Graham’s attempts to create a new company and terminated his employment. (ECF No. 15, PageID.231.)

2. Deleted and Lost Electronic Information

Defendant Graham was issued an Apple iPhone by Plaintiff for work purposes. (ECF No. 82-6, PageID.2468.) At some point shortly before his dismissal, he cleared all of the data from both his iPhone and the associated iCloud storage service.³ (*Id.*, PageID.2468-70 (“I recall wiping the iCloud account and wiping the phone.”).) This would have included all text messages and emails, if any, with Defendants Sheahan and Charnot.⁴ (*Id.*, PageID.2473-74.) According to Defendant Graham, he wiped his data because he stored “[a] lot of personal information on it” that he did not want to be shared; however, he claimed he retained at least some text messages “in case they needed to be used as evidence” since he was “contemplating legal action” against Plaintiff. (*Id.*, PageID.2469.)

³ A later forensic review would reveal that there was no data on the iPhone that predated June 29, 2020. (ECF No. 82, PageID.2409-10; ECF No. 82-7, PageID.2499-510.)

⁴ Defendant Charnot maintains his communication with Defendant Graham regarding security businesses was limited to phone calls and not typed messages of any sort, although he noted he would use text messages to “send jokes back and forth” to Defendant Graham. (ECF No. 82-3, PageID.2447-48.) According to Defendant Charnot, there is “nothing” related to the litigation in his phone. (*Id.*)

After his termination in July 2020, Defendant Graham acquired a new iPhone. (*Id.*, PageID.2480.) While he claims there “were no business contents” on this phone, his new iPhone was used to communicate with others regarding Great Lakes Security. (*Id.*, PageID.2486.) However, Defendant Graham was unsure whether communications with Defendants Sheahan and Charnot pertaining to either Great Lakes Security or Plaintiff existed in the iCloud associated with this new iPhone. (*Id.*, PageID.2485-87.) According to Defendant Graham, the new iPhone was either lost or stolen on January 8, 2021, and to “protect” his personal information, he again wiped his iCloud data “just to be safe.” (ECF No. 56-5; ECF No. 82-6, PageID.2481, 2485, 2490-91.) Additionally, in a remarkable run of bad luck, information possessed by Defendants other than Graham was utterly lost in a number of different ways. For example, Defendant Sheahan’s smartphone was purportedly water damaged in approximately July or August 2020, and consequently, the data on the device was lost. (ECF No. 82-2, PageID.2431-32.) Similarly, Defendant Charnot’s computer was hacked “a few months” before his August 2021 deposition, and the contents were not recoverable. (ECF No. 82-3, PageID.2448-49.)

B. Procedural History

On October 16, 2020, three months after Plaintiff’s filed its complaint, Plaintiff filed a motion for a preliminary injunction. (ECF No. 18.) After briefing and a two-day hearing, the court granted the motion on December 29, 2020. (ECF No. 35.) The court ordered Defendants to cease solicitation of Plaintiff’s clients and employees, and it directed Defendants to turn over any confidential information in Defendants’ possession. (ECF No. 35, PageID.1189-90.) Specifically, the court stated that Defendants must: 1)

return Plaintiff's confidential, proprietary and trade secret information; 2) preserve and produce all electronic devices used to view or retain Plaintiff's confidential, proprietary, and trade secret information for forensic analysis and remediation; 3) provide a verified written inventory of the information taken from Plaintiff. (*Id.*, PageID.1190.)

On May 18, 2021, after extensive briefing and a hearing (ECF Nos. 47, 51, 53, 56-59), the court, at Plaintiff's request, directed Defendants to show cause why they should not be held in contempt for violating the court's December 29 injunction. (ECF No. 60.) In the May 18 opinion, the court held that Defendants had failed to complete production of information as the court's previous order required. (See *id.* (citing ECF No. 35).) The May 18 order directed Defendants to complete ten discovery tasks to bring themselves into compliance with the December 29 injunction:

(1) produce any available forensic images of their computers as the computers existed prior to Defendants' expert accessing the computers by means of a USB drive; 2) produce the USB drives Defendants' expert used to access their computers; 3) provide a formal declaration signed by counsel stating whether Defendants retained copies of any data subject to the court's December 29 injunction; 4) produce an affidavit proving that, on November 5, 2020, Tech Shield performed a data transfer for Defendants' computers; 5) produce forensic copies of Defendants' computers; 6) secure and produce Defendant Graham's available iCloud data; 7) allow Avalon to lock-out Defendant Graham from access to his OneDrive account, to forensically capture the account and provide a filelisting report to all parties that includes all available file dates, and to produce a listing of all electronic devices authorized to use and/or upload to the OneDrive account; 8) allow Avalon to restore Defendant Graham's most recent Carbonite backup data to a blank computer, to screenshot the number of Carbonite backups available and their dates, and, when the most recent backup is restored, to produce to all parties a file-listing report of user files in Microsoft Excel format; 9) allow Avalon to produce file-listing reports for Defendant Graham's Google Drive account, tied to his personal Google email address, that includes all available file dates; 10) produce internet history reports for Defendants' computers.

(ECF No. 60, PageID.1674.)

On July 1, 2021, after providing Defendants an opportunity to respond, the court held that Defendants were in contempt of court for violating the December 29 injunction and the May 18 opinion. (ECF No. 69, PageID.1949-56.) The court ordered Defendants to complete production of information, in compliance with the December 29 injunction and May 18 opinion, by July 16, 2021. (*Id.*, PageID.1956.) Defendants, who had been given “numerous opportunities to . . . explain any justification for their non-compliance” (ECF No. 60, PageID.1672), were warned that if they “yet again fail[ed] to comply with the court’s order, the court will consider more severe sanctions.” (ECF No. 69, PageID.1956.)

The most disputed items of the May 18 order are ostensibly those which required production of forensic copies of Defendants’ devices. On July 23, 2021, a telephonic conference was held in which Defendants expressed concern that forensic copies would reveal privileged information on their computers. (ECF No. 78, PageID.2279-81.) Accordingly, the court permitted Defendants more time to comply with the order so that they could create a privilege log to protect any data outside the scope of discovery. Notably, at the conference, the court asked if Defendants could comply with a July 30, 2021, deadline for producing a privilege log and forensic copies of Defendants’ computers. (ECF No. 78, PageID.2275.) Counsel for Defendants stated “[t]hat is the hope,” but the court articulated that the deadline should be viewed as a “requirement and not a hope.” (*Id.*, PageID.2276.) On July 28, 2021, the court once more ordered in a text entry on the docket that Defendants “must produce forensic copies of their computers, with a privilege log, by July 30, 2021.”

The court met with the parties on August 19, 2021, to address ongoing discovery discrepancies. At this conference, the parties disputed whether many of the items in the order had been complied with and whether there were legitimate justifications for noncompliance.⁵ For instance, counsel for Plaintiff explained that forensic copies of Defendants' computers, the contents of which are crucial to the case, still had not been produced.⁶ (See, e.g., ECF No. 81, PageID.2384-85, 2389, 2391-92.) Defendants, represented by Lisa Stauff, proffered various excuses for their noncompliance with particular discovery requests; as to the forensic copies of the computers, Defendants ultimately admitted the forensic copies were not produced by July 30 as required. (ECF No. 81, PageID.2389) The court warned Defendants' counsel once again:

I think it should be clear, Ms. Stauff, that down this road with the kind of non-compliance that I am inclined to find has occurred thus far, we're not very many steps away from case dispositive sanctions for a failure to cooperate . . . meaningfully in the discovery process, subject to the Court's order[s]. . . . The possibility of case dispositive sanctions should . . . be recognized. And that will stand as a fair warning of the possible gravity of the situation at this point.

(ECF No. 81, PageID.2394.)

⁵ The parties had been instructed to file a joint statement on the state of Defendants' compliance with the court's orders two weeks before the conference; the parties filed separate statements, and Defendants' statement was two days late. (ECF No. 77.) At this time, the parties agreed only three of the items were completed without question: items 2, 8, and 10. (ECF Nos. 76, 77, 79.)

⁶ Plaintiffs have vehemently argued that the forensic copies of Defendants' devices are key evidence to the case due to Defendants' repeated failures to comply with the court's orders. Defendants have countered, arguing Plaintiff is "already in possession" of files that purport to give Plaintiff the information they need, but Plaintiff has made clear that "the purpose of the forensic imaging was that what the defendants have been forthcoming about has been shifting over time. They are completely unreliable as witnesses and as electronic discovery partners," and the forensic images would help reveal more about which critical files, if any, have been possessed or deleted in the past. (ECF No. 81, PageID.2382-85.)

To date, Defendants have not communicated to the court their compliance with—nor their intention to comply with—the uncompleted tasks set out in the May 18 order.⁷ Defendants have already been held in contempt for failing to cooperate with orders. (ECF No. 69, PageID.1949-56.) Additionally, they have not responded to the present motion before the court, which addresses whether Defendants should be sanctioned for “intentionally, willfully, and deliberately destroy[ing] evidence.” (ECF No. 82, PageID.2399.)

II. STANDARD

Before the Federal Rules of Civil Procedure were amended in 2015, courts required a party seeking sanctions for spoliation of evidence to establish that (1) the opposing party had control over the evidence and an “obligation to preserve it,” (2) the evidence was lost or destroyed with a “culpable state of mind,” and (3) the evidence was relevant to a claim or defense such that a “reasonable trier of fact could find that it would support that claim or defense.” See *Beaven v. U.S. Dep’t of Just.*, 622 F.3d 540, 553 (6th Cir. 2010). Following the amendments, however, courts generally require that the moving party satisfy the newly amended Rule 37(e) as it pertains to electronically stored information (“ESI”). See, e.g., *Applebaum v. Target Corp.*, 831 F.3d 740, 745 (6th Cir. 2016) (noting Rule 37(e) requires a showing of intent to justify an adverse inference jury instruction following lost ESI); *Courser v. Mich. House of Representatives*, 831 F. App’x 161, 187-88 (6th Cir. 2020) (explaining that “succeed[ing] on a Rule 37

⁷ Additionally, Plaintiff notes that Defendant Graham, in his deposition, testified that he sent Ms. Stauff text messages and other information related to his time with Plaintiff, but Defendants have allegedly still not produced this information. (ECF No. 82, PageID.2411 (citing ECF No. 82-6, PageID.2471).)

motion based on spoliation” now requires satisfying all of Rule 37(e)’s requirements);

Blasi v. United Debt Servs., LLC, No. 2:14-cv-83, 2020 WL 9597842, at *3 (S.D. Ohio

June 24, 2020) (observing the distinctions between the old and new standard for

spoliation sanctions). The amended rule states:

(e) Failure to Preserve Electronically Stored Information. If

electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information’s use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

Fed. R. Civ. P. 37(e).

Left undisturbed by the amendments is the court’s “broad discretion” in crafting spoliation sanctions under Rule 37(e)(1), *Beaven*, 622 F.3d at 553, although courts must take care that the sanctions constitute “measures no greater than necessary to cure the prejudice” and “do not have the effect of measures that are permitted under subdivision (e)(2).” See *Blasi*, 2020 WL 9597842, at *3 (quoting Fed. R. Civ. P. 37(e)(1), Advisory Comm. Notes (2015)). The most severe spoliation sanctions, such as an adverse inference instruction or entering default judgment, are appropriate only where there is a finding of intent; “[a] showing of negligence or even gross negligence will not

do the trick.” See *Applebaum*, 831 F.3d at 745; *Yoe v. Crescent Sock Co.*, No. 1:15-cv-3-SKL, 2017 WL 5479932, at *14 (E.D. Tenn. Nov. 14, 2017) (acknowledging that case dispositive sanctions are “the harshest sanctions” and are reserved for parties who acted with “intent to deprive another party of the information”).

III. DISCUSSION

A. Failure to Preserve ESI Under Rule 37(e)

Depending on a finding of an intentional deprivation of evidence, courts may proceed under either Rule 37(e)(1) or Rule 37(e)(2) in imposing a sanction for a party’s failure to preserve ESI; however, as a threshold matter, Rule 37(e) requires a showing that (1) the ESI was lost in “anticipation or conduct of litigation,” such that the party had a duty to preserve it; (2) the ESI was lost after the party “failed to take reasonable steps to preserve it”; and (3) the lost ESI “cannot be restored or replaced through additional discovery.” See *Konica Minolta Bus. Solutions, U.S.A. v. Lowery Corp.*, No. 15-CV-11254, 2016 WL 4537847, at *3, *5 (E.D. Mich. Aug. 31, 2016) (Roberts, J.) (“Defendants present compelling fact-based arguments as to why certain prerequisite elements of Rule 37(e) cannot be established, precluding the Court from turning attention to subsections (e)(1) and (e)(2).”).

1. Anticipation of Litigation

A party has a duty to preserve evidence for litigation “when that party has notice that the evidence is relevant to litigation or . . . should have known that the evidence may be relevant to future litigation.” See *John B. v. Goetz*, 531 F.3d 448, 459 (6th Cir. 2008) (internal quotations omitted); Fed. R. Civ. P. 37(e) Advisory Comm. Notes (2015) (explaining that Rule 37(e) applies where the “lost information should have been

preserved in the anticipation or conduct of litigation,” which “is based on [the] common-law duty” that requires “potential litigants . . . to preserve relevant information when litigation is reasonably foreseeable”). If, however, there was “no notice of pending litigation, the destruction of evidence does not point to consciousness of a weak case’ and intentional destruction.” *Beaven*, 622 F.3d at 553 (quoting *Kronsich v. United States*, 150 F.3d 112, 126 (2d Cir. 1998)). Rule 37(e) employs an “objective standard, viewed from the perspective of [Defendant] at the time that the [ESI] was destroyed.” *Freidig v. Target Corp.*, 329 F.R.D. 199, 207 (W.D. Wis. 2018) (citing *Trask-Morton v. Motel 6 Operating L.P.*, 534 F.3d 672, 681 (7th Cir. 2008)).

Here, all Defendants had a duty to preserve evidence. Plaintiff has produced email communications between and among Defendants that demonstrate full knowledge that litigation would soon be upon them. (ECF No. 82-4, PageID.2458.) In mid-June 2020, Defendants discussed how to “keep [Defendant Graham] anonymous as long as possible, and how to protect [him] from a non-compete suit that might come down the road.” (*Id.*) Moreover, Plaintiff presented an affidavit of one of Plaintiff’s vice presidents, James Howard, wherein Mr. Howard testified that Defendant Graham asked him to participate in a call with Defendants in June 2020 regarding the creation of a new, competing business. (ECF No. 18-2, PageID.526-27.) Notably, Defendant Graham had warned Mr. Howard they would “have to be careful” in creating a competing business. (*Id.*)

The evidence establishes Defendant Graham especially had reason to anticipate a future lawsuit as early as January 2020 when he submitted his application for a license to the IDFPR, specifically instructing the agency to “not contact [his] current

employer” because they would “fire [him] on the spot.” (See ECF Nos. 18-3, 18-4, 18-5, 18-6.) Moreover, Defendant Graham stated in his deposition that before deleting his Plaintiff-issued iPhone’s data and associated iCloud in June 2020, he was “contemplating legal action against [Plaintiff]” and consequently saved certain text messages “in case they needed to be used as evidence.”⁸ (ECF No. 82-6, PageID.2469.)

The court finds that all Defendants clearly had notice of future litigation and that they knew any evidence regarding their competing business would be evidence pertaining to a “non-compete suit that might come down the road.” (ECF No. 82-4, PageID.2458.) But some of the evidence that is now unobtainable was deleted even *after* the lawsuit was filed. Defendants Sheahan and Charnot were served with this action on July 7, 2020. (ECF Nos. 6, 10.) Defendant Sheahan broke his phone in approximately July or August 2020 and was unable to recover the data.⁹ (ECF No. 82-2, PageID.2431-32.) Defendant Charnot’s computer was hacked sometime before his August 2021 deposition, and the contents were not recoverable.¹⁰ (ECF No. 82-3,

⁸ According to Plaintiff, Defendants to this date have “still failed to inventory, produce or otherwise account for” these text messages that were saved by Defendant Graham. (ECF No. 82, PageID.2411.)

⁹ To the extent it could be argued Defendant Sheahan “broke” his phone before notice of the lawsuit, the court is convinced that Defendant Sheahan should have anticipated litigation long before June 2020 considering (1) Defendant Sheahan had met with Defendant Graham in approximately January 2020 to discuss how to organize Great Lake Security, (2) Defendants discussed the creation of the business ten to twenty times between March and July 2020, and (3) the record establishes Defendant Graham’s serious concern with being caught by his former employers creating a new business. (ECF No. 82-2, PageID.2435-36, 2438.)

¹⁰ Defendant Charnot was further under an express obligation to not lose any of the contents of his computer; the court’s injunction issued December 29, 2020, required Defendants to “preserve and produce” electronic devices used to “view or retain”

PageID.2448-49.) Therefore, having found there was ESI that “should have been preserved in the anticipation of litigation,” Defendants’ duty to preserve ESI—such as their electronic communications and documents—stored on their phones or computers within their control was triggered.

2. Reasonable Steps to Preserve ESI

The record establishes that Defendants failed to take reasonable steps to preserve ESI. As to Defendant Graham, not only did he twice delete all information on his iPhone, he further erased all data stored on his *iCloud*—the very mechanism that would have allowed him to wipe his phone of private or personal information while properly preserving data relevant to this litigation. (ECF No. 82-6, PageID.2468-70, 2482, 2488-89.) Indeed, after Defendant Graham’s iPhone was allegedly stolen, he failed to take the reasonable steps of using the phone’s geolocating features like “Find My iPhone,” nor did he make any inquiries to Apple to ensure the preservation of data. (ECF No. 82-6, PageID.2482, 2488-89.) As Plaintiff notes, this deletion occurred despite Apple’s features that allow a user to preserve data, including “(1) engaging an ‘Activation Lock’ to protect data on the missing phone, requiring an Apple ID and password to reactivate the iPhone; (2) disabling Apple Pay and any associated [financial information] . . . ; and (3) allowing the user ‘to restore the information on it with an existing backup’ from his iCloud.” (ECF No. 82, PageID.2417 (quoting an Apple Support webpage); ECF No. 82-8, PageID.2513.) Instead of taking steps to preserve

Plaintiff’s confidential information. (ECF No. 35, PageID.1190.) Given his recurring communication with Defendant Graham, it is reasonable to infer there was at least some evidence that was “relevant to litigation” on his computer. *See Dow Corning Corp. v. Weather Shield Mfg., Inc.*, 790 F. Supp. 2d 604, 616 (E.D. Mich. 2011) (Ludington, J.)

ESI, for a *second* time, he wiped all the data from his iCloud. (ECF No. 56-5; ECF No. 82-6, PageID.2481, 2490-91.)

Defendants Charnot and Sheahan both had notice of potential litigation yet “failed to exercise sufficient control of the data” they possessed. See *Yoe*, 2017 WL 5479932, at *10. Defendant Charnot lost all data on his computer, which he had used for three years, and left the device with a computer repair service despite being subject to an injunction for months that required him to preserve evidence on electronic devices. (ECF No. 82-3, PageID.244.) Beginning in January 2020, Defendant Sheahan was in frequent communication with Defendant Graham regarding a new, competing business leading up to the initiation of the lawsuit. (ECF No. 82-2, PageID.2435-36, 2438.) Despite their expectation of an impending noncompete claim, Defendants Charnot and Sheahan took “absolutely no steps to preserve the data” stored on their devices. *Id.* Thus, all Defendants failed to take “reasonable steps to preserve” the ESI over which they had control. Fed. R. Civ. P. 37(e).

3. Restoration or Replacement of Lost ESI

As previously noted, Plaintiff’s motion is unopposed. Defendants have not presented arguments as to whether the lost ESI could be restored or replaced through additional discovery; nonetheless, the record suggests that Plaintiff will ultimately be deprived of this information.

First, as to the data deleted by Defendant Graham in June 2020, he has admitted that to his knowledge, he is unable “to recreate an inventory of everything that was on the iCloud account.” (ECF No. 82-6, PageID.2474.) To the extent that he saved some of the ESI before wiping his iPhone and iCloud, Plaintiff maintains that “one year later,

Graham has still failed to inventory, produce or otherwise account for these documents.” (ECF No. 82, PageID.2412.) As it pertains to the ESI that Defendant Graham deleted in January 2021, Defendants themselves have admitted “[t]here is no iCloud account and no way to restore it,” and the contents are “irretrievable.” (ECF No. 56-5, PageID.1632.)

Likewise, Defendant Sheahan admitted he has been unable “to recover any contents on [his] phone.” (ECF No. 82-2, PageID.2432.) And Defendant Charnot was told the contents of his computer could not be recovered because “the computer was dead,” and he abandoned the device. (ECF No. 82-3, PageID.2448-49.) In sum, the lost ESI cannot be restored or replaced.

B. Sanctions Under Rule 37(e)(1) and (e)(2)

1. Intent to Deprive

Only upon a finding of an “intent to deprive another party” of ESI’s use in litigation may courts proceed under Rule 37(e)(2). *See Applebaum*, 831 F.3d at 745; *Culhane v. Wal-Mart Supercenter*, 364 F. Supp. 3d 768, 772-73 (E.D. Mich. 2019). “Courts should consider the extent to which a party was on notice that litigation was likely and that the information would be relevant.” *Culhane*, 364 F. Supp. 3d at 773 (quoting Fed. R. Civ. P. 37(e), Advisory Comm. Notes (2015)).

As to the intent of Defendants, the record shows without doubt that Defendant Graham acted with intent. Defendant Graham knew as early as January 2020—approximately seven months before his termination and the initiation of this action—litigation was on the horizon. This is clear from his specific requests that IDFPR not contact Plaintiff. (ECF No. 18-5, PageID.545.) Yet, since that time, Defendant Graham has completely erased all contents of both his iPhone and associated iCloud *twice*. The

first instance was mere days before his July 2020 termination by Plaintiff even though he knew the iPhone and iCloud contained communications with the other Defendants; he was aware that this information was significant. (ECF No. 82-6, PageID.2468-70.) The second instance was approximately January 8, 2021, a mere week after the court issued the December 29 injunction requiring preservation of all devices “used to view or retain Plaintiff’s” information. (ECF No. 35, PageID.1190; ECF No. 82-6, PageID.2481.) Even if the second iPhone was truly stolen as Defendant Graham claims, and that he erased the iCloud data “just to be safe,” the court agrees with Plaintiff that Graham’s professed reasoning is illogical: the major purpose of Apple’s service in providing an “iCloud backup” is to deal with the lost-phone possibility. The iCloud exists to “remotely preserve data on an iPhone if it becomes lost or stolen.” (ECF No. 82, PageID.2417; ECF No. 64-19, PageID.1799.) The most reasonable inference is that Graham’s erasures were sparked by an intent to conceal unfavorable information. Between his apprehension of being detected creating a new business or soliciting Plaintiff’s customers, and his repeated deletion of data, intentional destruction of evidence can be inferred. This warrants sanctions under Rule 37(e)(2).

Less clear is that Defendants Charnot and Sheahan acted with intent. It is true that Defendant Charnot claims to have lost all data on his computer, which he had used for years, and left the device with a computer repair service. He did so despite being subject to an injunction for months that required him to preserve it. (ECF No. 82-3, PageID.244.) Losing this information is more than negligent; considering that the information was lost *after* being subject to the court’s entirely clear December 29 injunction, it is accurately characterized as reckless. Likewise, Defendant Sheahan was

at least negligent given his recurring communication regarding the new, competing business with Defendant Graham leading up to the initiation of the lawsuit—he must have known about Defendant Graham's concern with being sued. (ECF No. 82-2, PageID.2435-36, 2438.) But still, a clear intent to deprive is lacking. Indeed, Plaintiff concedes that “[w]ith respect to Sheahan’s smartphone and Charnot’s computer,” it “cannot speak to [their] intentionality.” (ECF No. 82, PageID.2424.) Indeed, the court finds that unlike Defendant Graham, they did not act with an “intent to deprive” Plaintiff of ESI. Fed. R. Civ. P. 37(e)(2).

2. Prejudice

Having found no intent to deprive by Defendants Sheahan and Charnot, the court may still impose sanctions under Rule 37(e)(1) “upon finding prejudice to another party from loss of the information,” so long as the remedial measures are “no greater than necessary to cure the prejudice.” “‘Prejudice’ can be ‘properly understood as a party’s ability to obtain the proofs necessary for its case . . . which is another way of saying the loss of ESI could negatively impact a party’s ability to make its case, or prejudice that party because of the loss of information.’” *J.S.T. Corp. v. Robert Bosch LLC*, No. 15-13842, 2019 WL 2324488, at *6 (E.D. Mich. May 30, 2019) (quoting *Konica Minolta*, 2016 WL 4537847, at *3), *report and recommendation adopted*, No. 15-13842, 2019 WL 2296913 (E.D. Mich. May 30, 2019). Some courts have advanced the notion that that “[t]o show prejudice resulting from the spoliation, a party must only come forward with plausible, concrete *suggestions* as to what [the destroyed] evidence *might have been*.” See *Yoe*, 2017 WL 5479932, at *11 (quoting *TLS Mgmt. & Mktg. Servs. LLC v. Rodriguez-Toledo*, No. 15-2121, 2017 WL 1155743, at *1-2 (D.P.R. Mar. 27, 2017)).

See also Automated Solutions Corp. v. Paragon Data Sys., Inc., 756 F.3d 504, 514 (6th Cir. 2014) (citing *Beaven* and finding a party seeking sanctions “may rely on circumstantial evidence to suggest the contents of destroyed evidence”).

Here, it appears Defendants knew the ESI would be relevant to Plaintiff’s claims but failed to preserve it. Just before his termination, Defendant Graham deleted all of the contents of his iPhone and iCloud and says he has been unable to recover the lost contents. These would have included all text messages and emails with Defendants Sheahan and Charnot. (ECF No. 82-2, PageID.2435-36, 2438; ECF No. 82-6, PageID.2472-74.) The messages would have reasonably included evidence of his intention to breach his noncompete agreement or perhaps to solicit certain customers of Plaintiff. Relatedly, it is reasonable to assume that at least some contents of Defendant Charnot’s computer—which he used for more than three years leading up to the present case—could constitute evidence relevant to this action. (ECF No. 82-3, PageID.2448.) The same can be said for Defendant Sheahan, who was in communication about the formation of Great Lakes Security with the other Defendants since approximately January 2020. (ECF No. 82-2, PageID.2435-36, 2438.) In short, Plaintiff makes the case—and Defendants fail to dispute—that the evidence lost “would have been relevant to the contested issue” and that a “reasonable trier of fact could find that it would support that claim.” *Beaven*, 622 F.3d at 554-55.

But the prejudice to Plaintiff’s case also should be considered in light of Defendant’s compliance in this case. Defendants have repeatedly failed to produce, *inter alia*, forensic copies of electronic devices owned by Defendants, despite being required to do so by the court’s December 29 and May 18 orders. Forensic copies of

computers would be central to the Plaintiff's claim because it would help demonstrate exactly what information was possessed by Defendants—yet, for months, they have failed to produce them. (See e.g., ECF No. 79, PageID.2296 (“It is crucial to forensically analyze and remediate this computer because if Graham accessed OneDrive on the computer, then he could have accessed all Plaintiff's information.”).)

3. Imposition of Sanctions

In summary, Plaintiff has requested severe sanctions in this case—either default judgment or adverse inferences. (ECF No. 82, PageID.2398-99.) Between Defendants' disregard of the court's orders to produce discoverable information and their failure to preserve vital ESI, the court is inclined to find that sanctions are warranted for Defendants Charnot and Sheahan under Rule 37(e)(1) and for Defendant Graham under Rule 37(e)(2). In fact, while the court recognizes that case dispositive sanctions are sanctions of “last resort,” they may be necessary to impose against Defendant Graham under the circumstances. See, e.g., *Beil v. Lakewood Eng'g & Mfg. Co.*, 15 F.3d 546, 552 (6th Cir. 1994) (citing *Taylor v. Medtronics, Inc.*, 861 F.2d 980, 985 (6th Cir. 1988)). As to Defendants Sheahan and Charnot, the court is convinced they each had reason to expect noncompete litigation due to their ongoing communication with Defendant Graham and therefore failed to preserve ESI, prejudicing Plaintiff's case. Despite a strong showing that it is justified to issue Rule 37(e) sanctions against all Defendants, the court will issue an order to show cause to determine their propriety.

Additionally, as outlined below, the entry of default judgment against all Defendants appears proper pursuant to Rule 37(b). But the court will provide Defendants a final opportunity to be heard on this matter as well.

B. Rule 37(b) Sanctions

The Federal Rules of Civil Procedure provide that a court has authority to sanction a party where the “party or a party’s officer, director, or managing agent . . . fails to obey an order to provide or permit discovery.” Fed. R. Civ. P. 37(b)(2)(A). The rule permits, among other sanctions, dismissing a case, granting judgment, or holding a party in contempt. See *id.* Although Plaintiff brought sanctions for the spoliation of evidence only, case law supports the court’s ability to bring Rule 37(b) sanctions *sua sponte*. See *Chambers v. NASCO, Inc.*, 501 U.S. 32, 42 n. 8 (1991) (enumerating Federal Rules of Civil Procedure, including Rule 37, which “provide for the imposition of attorney’s fees as a sanction,” and finding that courts “generally may act *sua sponte* in imposing sanctions under the Rules.”). See also *Dreith v. Nu Image, Inc.*, 648 F.3d 779, 787 (9th Cir. 2011) (“These failures to comply with orders of the court provided [the district court] with the power under Rule 37(b) to impose sanctions *sua sponte*, up to and including default.”); *Elmore v. City of Greenwood*, No. 313-cv-01755-TLW-KDW, 2015 WL 3868068, at *5 (D.S.C. June 23, 2015) (collecting cases permitting the *sua sponte* issuance of sanctions under Rule 37).

Case dispositive sanctions may be warranted where “the party’s failure to cooperate in discovery was willful, in bad faith, or due to its own fault.” *Beil*, 15. F.3d at 552 (citing *Taylor v. Medtronics, Inc.*, 861 F.2d 980, 985 (6th Cir. 1988)). In determining whether sanctions under Rule 37(b) are appropriate, courts consider three factors: “(1) whether the adversary was prejudiced by the . . . party’s failure to cooperate in discovery, (2) whether the . . . party was warned that failure to cooperate could lead to

dismissal, and (3) whether less drastic sanctions were imposed or considered before dismissal was ordered.” *Id.* (quoting *Taylor*, 861 F.2d at 986).

As an initial matter, it is necessary to reiterate that Defendants have repeatedly failed to abide by the court’s discovery orders. For example, Defendants were ordered in a December 2019 injunction to “preserve and produce all electronic devices used to view or retain Plaintiff’s confidential, proprietary, and trade secret information for forensic analysis and remediation.” (ECF No. 35, PageID.1190.) As noted above in the court’s Rule 37(e) analysis, Defendants failed to comply with this order. But further, to bring Defendants into compliance with the injunction, the court issued the May 18 order requiring Defendants to complete discovery tasks, including an obligation to “produce forensic copies of Defendants’ computers” and “secure and produce Defendant Graham’s available iCloud data.” (ECF No. 60, PageID.1675.) Later, on July 1, 2021, having found “numerous, detailed reports of Defendants’ failure to comply” with the court’s orders, the court following a hearing determined Defendants were in contempt of court. (ECF No. 69, Page.1956.) Again, Defendants were ordered to complete all ten items of discovery by July 16, but the court subsequently permitted Defendants to create a privilege log and accordingly extended the deadline to July 30 in both a status conference (ECF No. 78, PageID.2275-76) and a text entry on the docket dated July 28, 2021. And again, when the court addressed the ongoing discovery discrepancies in status conference on August 19, 2021, it was clear that many of the items—such as the forensic copies of the computers with a privilege log—were not completed. (ECF No. 81, PageID.2388-90.) Still, to this date, there is no indication that all of the requirements of the May 18 order have been accomplished.

But Defendants' ostensible defiance does not end there. Defendants were ordered to "provide a formal declaration signed by counsel stating whether Defendants retained copies of any data subject to the court's December 29 injunction." (ECF No. 60, PageID.1675.) They produced this document; Defendants' counsel on June 15, 2021, submitted a declaration that stated "Defendants, in their own right or through agents, retain no copies of any data (Prudential's or otherwise) from Mr. Graham's computers." (ECF No. 64-7, PageID.1757.) However, the record suggests the opposite. Defendant Graham testified in his deposition that he sent text messages between himself and Plaintiff's employees as well as information pertaining to one of Plaintiff's clients to Ms. Stauff in approximately August or September 2020 (ECF No. 82-6, PageID.2470); the court is persuaded by Plaintiff—and Defendants have failed to contest—that over a year later, Defendants have not accounted for this information.¹¹ (ECF No. 79-2, PageID.2313-16; ECF No. 82, PageID.2411.)

Given Defendants' persistent disobedience with the court's orders and their failure to meaningfully cooperate with Plaintiff, the court is inclined to impose case dispositive sanctions against Defendants; all three factors support this conclusion.

1. Prejudice

First, the record establishes Plaintiff would be prejudiced by Defendants' continued discovery abuses. As Plaintiff has noted, it is clear that Defendants have not been "forthcoming about all the data and data manipulation reflected on" their electronic

¹¹ As to the documents that Defendant Graham sent to Ms. Stauff, Ms. Stauff represented to the court that she "hoped to produce these documents (all in electronic form) to supplement discovery responses . . . but there has been no time." (ECF No. 77, PageID.2113.) Still, these documents have not been produced.

devices, which is precisely why “forensic copies of the computers—including their deleted files—are necessary.” (ECF No. 79, PageID.2298.) The success of the substantive claims brought by Plaintiff depends significantly on determining what trade secret information was possessed by Defendants and to what extent it was used in an attempt to compete with Plaintiff. By deleting ESI, failing to turn over documents that are related to the litigation, and refusing to produce forensic copies of devices that could aid in verifying what was possessed or deleted, Plaintiff is severely prejudiced in its ability to succeed on its claims. Plaintiff has requested—and the court has ordered numerous times—that Defendants complete these discovery items, but they have refused to cooperate.

2. Warnings

Second, Defendants were unequivocally warned that the court would consider granting judgment in favor of Plaintiff as a result of its ongoing discovery abuses. In its order dated July 1, 2021, which determined Defendants were in contempt of court, the court explained that if Defendants “yet again fail to comply with the court’s orders, the court will consider more severe sanctions to effect compliance.” (ECF No. 69, PageID.1956.) One month later, after it seemed as though Defendants had continued to fail to cooperate in discovery, the court further warned Defendants’ counsel “it should be clear . . . that down this road with the kind of non-compliance that I am inclined to find has occurred thus far, we’re not very many steps away from case dispositive sanctions for a failure to cooperate . . . meaningfully in the discovery process, subject to the Court’s order[s].” (ECF No. 81, PageID.2394.) Defendants were given a “fair warning” of

the gravity of the situation, and the court *expressly* informed Defendants’ counsel that “[t]he possibility of case dispositive sanctions should . . . be recognized.” (*Id.*)

3. Less Drastic Sanctions

Finally, less drastic sanctions have already been considered and imposed. As noted, the court previously held Defendants in contempt after it found “numerous, detailed reports of Defendants’ failure to comply” with the court’s orders—it appears nothing has changed. (ECF No. 60, PageID.1672). The court even discussed alternative methods of ensuring compliance with Defendants’ counsel at the August 19 conference:

THE COURT: Ms. Stauff, what do you suggest the Court can do to, to not any longer encourage but to require compliance?

MS. STAUFF: Your Honor, the Court has been requiring compliance, and Defendants are complying. The problem is that the list keeps changing.

(ECF No. 81, PageID.2388). The “list” has never changed. The court’s orders regarding ESI and forensic copies of Defendants’ computers have remained the same since the December 29 injunction (ECF No. 35), the May 18 opinion (ECF No. 60), the July 1 opinion (ECF No. 69), the July 23 oral ruling (ECF No. 78, PageID.2274-76), and the July 28 text order. Defendants’ counsel, instead of suggesting less drastic sanctions to the court, asserted Defendants have been complying with the court’s discovery orders. But Defendants’ claim of compliance is demonstrably untrue. For example, Defendant Graham’s deletion of his iCloud data—a *week after* the December 29 injunction required him to preserve the type of information that would be found on it—falls far short of “complying” with court orders. (ECF No. 35, PageID.1190; ECF No. 82-6, PageID.2481.) It seems any further attempts to guarantee cooperation in discovery would be futile.

Thus, the court is inclined to impose case dispositive sanctions against all Defendants pursuant to Rule 37(b). Nonetheless, the court will issue an order to show cause to afford Defendants one final opportunity to apprise the court of any compliance with discovery orders and to refute the contentions in Plaintiff's motion seeking sanctions for spoliation. (ECF No. 82.)

IV. CONCLUSION

The court is cognizant that dispositive sanctions are sanctions of last resort. But the law supports such sanctions against a party where "failure to cooperate in discovery was willful, in bad faith, or due to its own fault." *Beil*, 15 F.3d at 552. Defendants' conduct very well may warrant the entry of a default judgment, but they will have a further opportunity to be heard on the matter. Accordingly,

IT IS ORDERED that Plaintiff's "Motion for Sanctions for Defendants' Spoliation of Evidence" (ECF No. 82) is GRANTED IN PART.

IT IS FURTHER ORDERED that Defendants are DIRECTED to show cause, in writing, by **November 8, 2021**, why sanctions should not be imposed against them pursuant to Rule 37(b) or Rule 37(e). Defendants should take care to address the propriety of an entry of default judgment.

s/Robert H. Cleland /
ROBERT H. CLELAND
UNITED STATES DISTRICT JUDGE

Dated: October 15, 2021

I hereby certify that a copy of the foregoing document was mailed to counsel of record on this date, October 15, 2021, by electronic and/or ordinary mail.

s/Lisa Wagner /
Case Manager and Deputy Clerk
(810) 292-6522